

Characterization of Negabent Functions and Construction of Bent-Negabent Functions with Maximum Algebraic Degree

Wei Su, Alexander Pott, and Xiaohu Tang

Abstract

We present necessary and sufficient conditions for a Boolean function to be a negabent function for both even and odd number of variables, which demonstrate the relationship between negabent functions and bent functions. By using these necessary and sufficient conditions for Boolean functions to be negabent, we obtain that the nega spectrum of a negabent function has at most 4 values. We determine the nega spectrum distribution of negabent functions. Further, we provide a method to construct bent-negabent functions in n variables (n even) of algebraic degree ranging from 2 to $\frac{n}{2}$, which implies that the maximum algebraic degree of an n -variable bent-negabent function is equal to $\frac{n}{2}$. Thus, we answer two open problems proposed by Parker and Pott and by Stănică *et al.* respectively.

Index Terms

Boolean function, bent function, negabent function, bent-negabent function, Walsh-Hadamard transform, nega-Hadamard transform.

I. INTRODUCTION

Boolean functions play an important role in cryptography and error-correcting codes. They should satisfy several properties, which are quite often impossible to be satisfied simultaneously. One of the most important requirements for Boolean functions is the nonlinearity, which means that the function is as far away from all affine functions as possible. In 1976, Rothaus introduced the class of *bent functions* which have the maximum nonlinearity [1]. These functions exist only on even number of variables and an n -variable bent function can have degree at most $\frac{n}{2}$.

A Boolean function is bent if and only if its spectrum with respect to the Walsh-Hadamard transform is flat (i.e. all spectral values have the same absolute value). Parker and Riera extended the concept of a bent function to some generalized bent criteria for a Boolean function in [2], [3], where they required that a Boolean function has flat spectrum with respect to one or more transforms from a specified set of unitary transforms. The set of transforms they chose is not arbitrary but is motivated by a choice of local unitary transforms that are central to the structural analysis of pure n -qubit stabilizer quantum states. The transforms they applied are n -fold tensor products

W. Su and X. Tang are with the Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, 610031, China. Su is currently a visiting Ph.D. student of the Institute for Algebra and Geometry (IAG), Otto-von-Guericke University Magdeburg, D-39106 Magdeburg, Germany. (e-mail: weisu0109@googlemail.com, xhutang@ieee.org)

A. Pott is with the Institute for Algebra and Geometry (IAG), Otto-von-Guericke University Magdeburg, D-39106 Magdeburg, Germany. (e-mail: alexander.pott@ovgu.de)

of the identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the Walsh-Hadamard matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and the nega-Hadamard matrix $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, where $i^2 = -1$. The Walsh-Hadamard transform can be described as the tensor product of several H 's, and the nega-Hadamard transform is constructed from the tensor product of several N 's. As in the case of the Walsh-Hadamard transform, a Boolean function is called *negabent* if the spectrum under the nega-Hadamard transform is flat.

There are some papers in the area of negabent functions in the last few years [4]-[8]. An interesting topic is to construct Boolean functions which are both bent and negabent (*bent-negabent*), whose results are listed as follows.

- 1) In [4], Parker and Pott gave necessary and sufficient conditions for quadratic functions to be bent-negabent. It turns out that such quadratic bent-negabent functions exist for all even n . They also described all Maiorana-McFarland type bent functions which are simultaneously negabent. It seems difficult to apply this result in order to construct Maiorana-McFarland bent-negabent functions. For even number of variables, necessary and sufficient condition for a Boolean function to be a negabent function has also been presented. In [4], they proposed the following open problem (open problem 3 in [4]).

Open Problem 1: Find the maximum degree of bent-negabent functions.

- 2) In [5], transformations that leave the bent-negabent property invariant are presented. A construction for infinitely many bent-negabent Boolean functions in $2mn$ variables ($m \not\equiv 1 \pmod{3}$) and of algebraic degree at most n is described, this being a subclass of the Maiorana-McFarland bent class. Moreover, the algebraic degrees of n -variable bent-negabent functions in this construction are less than or equal to $\frac{n}{4}$ and $n \equiv 0 \pmod{4}$. Finally it is shown that a bent-negabent function in n (n even) variables from the Maiorana-McFarland class has algebraic degree at most $\frac{n}{2} - 1$, but not an existence result.
- 3) In [6], Stănică *et al.* developed some properties of nega-Hadamard transforms. Consequently, they derived several results on negabentness of concatenations, and partially-symmetric functions. They also obtained a characterization of bent-negabent functions in a subclass of Maiorana-McFarland set.
- 4) In [7], Stănică *et al.* pointed out that the algebraic degree of an n -variable negabent function is at most $\lceil \frac{n}{2} \rceil$. Further, a characterization of bent-negabent functions was obtained within a subclass of the Maiorana-McFarland set. They developed a technique to construct bent-negabent Boolean functions by using complete mapping polynomials. Using this technique they demonstrated that for each $l \geq 2$ there exist bent-negabent functions on $n = 12l$ variables with algebraic degree $\frac{n}{4} + 1 = l + 1$. It is also demonstrated that there exist bent-negabent functions on 8 variables with algebraic degrees 2, 3 or 4. Moreover, they presented the following open problem.

Open Problem 2: For any $n \equiv 0 \pmod{4}$, give a general construction of bent-negabent Boolean functions on n variables with algebraic degree strictly greater than $\frac{n}{4} + 1$.

- 5) In [8], Sarkar considered negabent Boolean functions defined over finite fields. He characterized negabent quadratic monomial functions. He also presented necessary and sufficient condition for a Maiorana-McFarland bent function to be a negabent function. As a consequence of that result he can obtain bent-negabent Maiorana-McFarland function of degree $\frac{n}{4}$ over \mathbb{F}_{2^n} .

In this paper, we concentrate on negabent functions and bent-negabent functions. In particular, we have the

following contributions.

- In Section III, direct links between the nega-Hadamard transform and the Walsh-Hadamard transform are explored. By using this property, we study necessary and sufficient conditions for a Boolean function to be negabent for both even and odd number of variables, which demonstrate the relationship between negabent functions and bent functions.
- In Section IV, we obtain that the nega spectrum of a negabent function has at most 4 values. Hereafter, we determine the nega spectrum distribution of negabent functions.
- In Section V, we give a method to construct bent-negabent functions in n variables (n even) of degree ranging from 2 to $\frac{n}{2}$. These functions belong to the Maiorana-McFarland complete class. Thus, we can obtain that the maximum algebraic degree of an n -variable bent-negabent function is equal to $\frac{n}{2}$. Therefore, we answer the Open Problems 1 and 2 proposed in [4] and [7] respectively.

II. PRELIMINARIES

Let n be a positive integer, \mathbb{F}_2^n be the n -dimensional vector space over the two element field \mathbb{F}_2 . The set of integers, real numbers and complex numbers are denoted by \mathbb{Z} , \mathbb{R} and \mathbb{C} , respectively. To avoid confusion, we denote the addition over \mathbb{Z} , \mathbb{R} and \mathbb{C} by $+$, and the addition over \mathbb{F}_2^n by \oplus for all $n \geq 1$.

Let \mathcal{B}_n be the set of all maps from \mathbb{F}_2^n to \mathbb{F}_2 . Such a map is called an n -variable Boolean function. Let $f(x) \in \mathcal{B}_n$, the *support* of $f(x)$ is defined as $\text{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. The *Hamming weight* $\text{wt}(f)$ of $f(x)$ is the size of $\text{supp}(f)$, i.e., $\text{wt}(f) = |\text{supp}(f)|$. The *Hamming weight* of a binary vector $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$ is defined by $\text{wt}(x) = \sum_{i=1}^n x_i$. Each n -variable Boolean function $f(x)$ has a unique representation by a multivariate polynomial over \mathbb{F}_2 , called the *algebraic normal form (ANF)*:

$$f(x_1, \dots, x_n) = \bigoplus_{u=(u_1, u_2, \dots, u_n) \in \mathbb{F}_2^n} f_u \prod_{i=1}^n x_i^{u_i}, \quad f_u \in \mathbb{F}_2.$$

The algebraic degree, $\deg(f)$, of f is defined as $\max\{\text{wt}(u) \mid f_u \neq 0, u \in \mathbb{F}_2^n\}$.

The *Walsh-Hadamard transform* of $f(x) \in \mathcal{B}_n$ at any vector $u \in \mathbb{F}_2^n$ is defined by

$$W_f(u) = 2^{-\frac{n}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + u \cdot x},$$

Here $u \cdot x$ is a usual inner product of vectors, i.e., $u \cdot x = u_1 x_1 \oplus u_2 x_2 \oplus \dots \oplus u_n x_n$ for $u = (u_1, u_2, \dots, u_n)$ and $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$. The *Walsh spectrum* of f consists of all values $\{W_f(u) \mid u \in \mathbb{F}_2^n\}$.

A function $f \in \mathcal{B}_n$ is said to be *bent* if $|W_f(u)| = 1$ for all $u \in \mathbb{F}_2^n$. It is *semibent* if $|W_f(u)| \in \{0, \pm\sqrt{2}\}$. Boolean bent (resp. semibent) functions exist only if the number of variables, n , is even (resp. odd). If $f \in \mathcal{B}_n$ is bent, then the *dual function* \tilde{f} of f , defined on \mathbb{F}_2^n by:

$$W_{\tilde{f}}(u) = (-1)^{\tilde{f}(u)}, \quad \forall u \in \mathbb{F}_2^n,$$

is also bent and its own dual is f itself.

The *autocorrelation* of f at u is defined as

$$C_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus u)}.$$

For even n , it is known that a function $f \in \mathcal{B}_n$ is bent if and only if $C_f(u) = 0$ for all $u \neq (0, 0, \dots, 0) \in \mathbb{F}_2^n$.

The *nega-Hadamard transform* of $f(x) \in \mathcal{B}_n$ at $u \in \mathbb{F}_2^n$ is the complex valued function:

$$N_f(u) = 2^{-\frac{n}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + u \cdot x} i^{\text{wt}(x)}.$$

The *nega spectrum* of f consists of all values $\{N_f(u) \mid u \in \mathbb{F}_2^n\}$.

A function is said to be *negabent* if $|N_f(u)| = 1$ for all $u \in \mathbb{F}_2^n$. Note that all the affine functions (both even and odd numbers of variables) are negabent [4]. For even number of variables, if a negabent function is also a bent function, then we call this function *bent-negabent*.

Define the *nega-autocorrelation* of f at $u \in \mathbb{F}_2^n$ by

$$c_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus u)} (-1)^{u \cdot x}.$$

In [6], it was shown that a Boolean function is negabent if and only if all its nontrivial nega-autocorrelation values are 0 which is analogous to the result concerning the autocorrelation values of a bent function.

We conclude this section by introducing the following notations which will be used throughout this paper.

- 1) $\mathbf{0}_n = (0, 0, \dots, 0)$ and $\mathbf{1}_n = (1, 1, \dots, 1) \in \mathbb{F}_2^n$;
- 2) $e_j : e_j \in \mathbb{F}_2^n$ denotes the vector of Hamming weight 1 with 1 on the j -th component;
- 3) $\bar{z} : \text{if } z = (z_1, \dots, z_n) \in \mathbb{F}_2^n$, then $\bar{z} = z \oplus \mathbf{1}_n$ denotes the bitwise complement of z ;
- 4) $|z| : \text{if } z = a + bi \in \mathbb{C}$ is a complex number, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z ;
- 5) $\sigma_d(x) : \text{if } x \in \mathbb{F}_2^n$, then $\sigma_d(x)$ denotes the elementary symmetric Boolean function on n variables with degree d ($1 \leq d \leq n$), i.e.,

$$\sigma_d(x) = \bigoplus_{1 \leq i_1 < \dots < i_d \leq n} x_{i_1} x_{i_2} \dots x_{i_d}, \quad \forall x = (x_1, \dots, x_n) \in \mathbb{F}_2^n.$$

In particular, if $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$, then $\sigma_1(x) = x_1 \oplus \dots \oplus x_n = \mathbf{1}_n \cdot x$ and $\sigma_2(x) = \bigoplus_{1 \leq i < j \leq n} x_i x_j$;

- 6) $GL(n, \mathbb{F}_2) : \text{the group of all invertible } n \times n \text{ matrices over } \mathbb{F}_2$.

III. CONNECTIONS BETWEEN NEGABENT FUNCTIONS AND BENT FUNCTIONS

In this section, direct links between the nega-Hadamard transform and the Walsh-Hadamard transform are explored. By using this property, we study necessary and sufficient conditions for a Boolean function to be negabent for both even and odd number of variables, which demonstrate the relationship between negabent functions and bent functions.

Lemma 1: Let $f \in \mathcal{B}_n$. Between the nega-Hadamard transform and the Walsh-Hadamard transform there is the relation

$$N_f(u) = \frac{W_{f \oplus \sigma_2}(u) + W_{f \oplus \sigma_2}(\bar{u})}{2} + i \cdot \frac{W_{f \oplus \sigma_2}(u) - W_{f \oplus \sigma_2}(\bar{u})}{2}.$$

Proof: First for any $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$, it can be easily proved by induction that

$$\text{wt}(x) \pmod{4} = \bigoplus_{i=1}^n x_i + 2 \bigoplus_{1 \leq i < j \leq n} x_i x_j = \sigma_1(x) + 2\sigma_2(x) = \mathbf{1}_n \cdot x + 2\sigma_2(x).$$

Thus, the nega-Hadamard transform of f at $u \in \mathbb{F}_2^n$ is

$$N_f(u) = 2^{-\frac{n}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + u \cdot x} i^{\text{wt}(x)} = 2^{-\frac{n}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \sigma_2(x) + u \cdot x} i^{\mathbf{1}_n \cdot x}.$$

Applying the formula $i^a = \frac{1+(-1)^a}{2} + i \cdot \frac{1-(-1)^a}{2}$ for $a \in \mathbb{F}_2$, we get

$$\begin{aligned} N_f(u) &= 2^{-\frac{n}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \sigma_2(x) + u \cdot x} \left[\frac{1 + (-1)^{\mathbf{1}_n \cdot x}}{2} + i \cdot \frac{1 - (-1)^{\mathbf{1}_n \cdot x}}{2} \right] \\ &= \frac{W_{f \oplus \sigma_2}(u) + W_{f \oplus \sigma_2}(u \oplus \mathbf{1}_n)}{2} + i \cdot \frac{W_{f \oplus \sigma_2}(u) - W_{f \oplus \sigma_2}(u \oplus \mathbf{1}_n)}{2} \\ &= \frac{W_{f \oplus \sigma_2}(u) + W_{f \oplus \sigma_2}(\bar{u})}{2} + i \cdot \frac{W_{f \oplus \sigma_2}(u) - W_{f \oplus \sigma_2}(\bar{u})}{2}. \end{aligned}$$

□

This property is an important tool to analyse the properties of negabent functions. If n is even, necessary and sufficient conditions for a Boolean function $f \in \mathcal{B}_n$ to be negabent has been given in [4]. By using Lemma 1 and the Jacobi's two-square theorem, we can obtain the necessary and sufficient conditions for a Boolean function $f \in \mathcal{B}_n$ to be negabent for both even and odd n . For completeness, we also provide the proofs for even n here.

Fact 1: (Jacobi's two-square theorem) Let k be a nonnegative integer.

- (1) The Diophantine equation $x^2 + y^2 = 2^{2k+1}$ has a unique nonnegative integer solution as $(x, y) = (2^k, 2^k)$.
- (2) The Diophantine equation $x^2 + y^2 = 2^{2k}$ has exactly two nonnegative integer solutions as $(x, y) = (2^k, 0)$ and $(x, y) = (0, 2^k)$.

Theorem 1: ([4]) Let n be even and $f(x) \in \mathcal{B}_n$. Then $f(x)$ is negabent if and only if $f(x) \oplus \sigma_2(x)$ is bent.

Proof: A Boolean function $f \in \mathcal{B}_n$ is negabent if and only if $|N_f(u)| = 1$ for all $u \in \mathbb{F}_2^n$. By Lemma 1, we have

$$|N_f(u)|^2 = \frac{(W_{f \oplus \sigma_2}(u))^2 + (W_{f \oplus \sigma_2}(\bar{u}))^2}{2} = 1, \quad \forall u \in \mathbb{F}_2^n,$$

hence,

$$(2^{\frac{n}{2}} W_{f \oplus \sigma_2}(u))^2 + (2^{\frac{n}{2}} W_{f \oplus \sigma_2}(\bar{u}))^2 = 2^{n+1}, \quad \forall u \in \mathbb{F}_2^n.$$

From Jacobi's two-square theorem we know that 2^{n+1} has a unique representation as a sum of two squares, namely $2^{n+1} = (2^{\frac{n}{2}})^2 + (2^{\frac{n}{2}})^2$ if n is even. Thus, it is equivalent to

$$|2^{\frac{n}{2}} W_{f \oplus \sigma_2}(u)| = |2^{\frac{n}{2}} W_{f \oplus \sigma_2}(\bar{u})| = 2^{\frac{n}{2}}, \quad \forall u \in \mathbb{F}_2^n,$$

i.e.,

$$|W_{f \oplus \sigma_2}(u)| = |W_{f \oplus \sigma_2}(\bar{u})| = 1, \quad \forall u \in \mathbb{F}_2^n.$$

This completes the proof. □

By Theorem 1, the following corollary is obvious.

Corollary 1: ([4]) If f is a bent-negabent function, then $f \oplus \sigma_2$ is also bent-negabent.

If n is odd, we can get a similar equivalent condition as for even n . In the following, we give three equivalent conditions of a Boolean function to be negabent for an odd number of variables. The latter two conditions show the relationship between n -variable negabent functions and $(n-1)$ -variable (or $(n+1)$ -variable) bent functions.

Theorem 2: Let n be odd and $f(x) \in \mathcal{B}_n$. Then the following statements are equivalent:

- (1) $f(x)$ is negabent;
- (2) $f(x) \oplus \sigma_2(x)$ is semibent and $|W_{f \oplus \sigma_2}(u)| \neq |W_{f \oplus \sigma_2}(\bar{u})|$ for all $u \in \mathbb{F}_2^n$;

- (3) $(f \oplus \sigma_2)(x_1, \dots, x_{n-1}, x_1 \oplus x_2 \oplus \dots \oplus x_n) = (1 \oplus x_n)g(x_1, \dots, x_{n-1}) \oplus x_n h(x_1, \dots, x_{n-1})$, where g and h are both bent functions with $(n-1)$ variables;
- (4) $f(x) \oplus \sigma_2(x) \oplus \sigma_1(x)y$ is bent in $n+1$ variables, where $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2$.

Proof: (1) \Leftrightarrow (2): A Boolean function $f \in \mathcal{B}_n$ is negabent if and only if $|N_f(u)| = 1$ for all $u \in \mathbb{F}_2^n$. It follows from Lemma 1 that

$$|N_f(u)|^2 = \frac{(W_{f \oplus \sigma_2}(u))^2 + (W_{f \oplus \sigma_2}(\bar{u}))^2}{2} = 1, \quad \forall u \in \mathbb{F}_2^n,$$

hence,

$$(2^{\frac{n}{2}} W_{f \oplus \sigma_2}(u))^2 + (2^{\frac{n}{2}} W_{f \oplus \sigma_2}(\bar{u}))^2 = 2^{n+1}, \quad \forall u \in \mathbb{F}_2^n.$$

By Jacobi's two-square theorem, it is equivalent to

$$\{|W_{f \oplus \sigma_2}(u)|, |W_{f \oplus \sigma_2}(\bar{u})|\} = \{0, \sqrt{2}\}, \quad \forall u \in \mathbb{F}_2^n.$$

According to the definition of semibent, we can obtain (1) is equivalent to (2).

(1) \Leftrightarrow (3): Let $f_1(x) = f(x) \oplus \sigma_2(x)$, $f_2(x) = (f \oplus \sigma_2)(x_1, \dots, x_{n-1}, x_1 \oplus x_2 \oplus \dots \oplus x_n)$, and the decomposition of $f_2(x)$ is $f_2(x) = (1 \oplus x_n)g(x_1, \dots, x_{n-1}) \oplus x_n h(x_1, \dots, x_{n-1})$ for some $g, h \in \mathcal{B}_{n-1}$. Then, for any $v = (v_1, \dots, v_{n-1}, v_n) \in \mathbb{F}_2^n$, we have

$$\begin{aligned} W_{f_2}(v) &= 2^{-\frac{n}{2}} \sum_{x' \in \mathbb{F}_2^{n-1}, x_n \in \mathbb{F}_2} (-1)^{(1 \oplus x_n)g(x') \oplus x_n h(x') \oplus v' \cdot x' \oplus v_n x_n} \\ &= 2^{-\frac{n}{2}} \sum_{x' \in \mathbb{F}_2^{n-1}} [(-1)^{g(x') \oplus v' \cdot x'} + (-1)^{v_n} (-1)^{h(x') \oplus v' \cdot x'}] \\ &= \frac{1}{\sqrt{2}} [2^{-\frac{n-1}{2}} \sum_{x' \in \mathbb{F}_2^{n-1}} (-1)^{g(x') \oplus v' \cdot x'} + (-1)^{v_n} 2^{-\frac{n-1}{2}} \sum_{x' \in \mathbb{F}_2^{n-1}} (-1)^{h(x') \oplus v' \cdot x'}] \\ &= \frac{1}{\sqrt{2}} [W_g(v') + (-1)^{v_n} W_h(v')], \end{aligned} \tag{1}$$

where $x' = (x_1, \dots, x_{n-1})$ and $v' = (v_1, \dots, v_{n-1}) \in \mathbb{F}_2^{n-1}$. Let Λ be an $n \times n$ matrix over \mathbb{F}_2 of the form

$$\Lambda = \begin{pmatrix} 1 & & & 1 \\ & 1 & & 1 \\ & & \ddots & \vdots \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix},$$

where “empty” entries are 0. Then $\Lambda^{-1} = \Lambda$ and $f_2(x) = f_1(x\Lambda)$. Therefore, for any $v \in \mathbb{F}_2^n$, we can get that

$$\begin{aligned} W_{f_2}(v) &= 2^{-\frac{n}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x\Lambda) \oplus v \cdot x} = 2^{-\frac{n}{2}} \sum_{y \in \mathbb{F}_2^n} (-1)^{f_1(y) \oplus v(y\Lambda)^T} \\ &= 2^{-\frac{n}{2}} \sum_{y \in \mathbb{F}_2^n} (-1)^{f_1(y) \oplus (v\Lambda^T) \cdot y} \\ &= W_{f_1}(v\Lambda^T), \end{aligned} \tag{2}$$

where the superscript T represents the transpose of a matrix.

For any $u = (u_1, \dots, u_{n-1}, u_n) \in \mathbb{F}_2^n$, denote $w = u\Lambda^T = (w_1, \dots, w_{n-1}, w_n) \in \mathbb{F}_2^n$. By equality (2), we have

$$W_{f_1}(u) = W_{f_2}(u(\Lambda^T)^{-1}) = W_{f_2}(u\Lambda^T) = W_{f_2}(w),$$

since $(\Lambda^T)^{-1} = \Lambda^T$. Combined with equality (1), we get

$$W_{f_1}(u) = W_{f_2}(w) = \frac{1}{\sqrt{2}}[W_g(w') + (-1)^{w_n}W_h(w')], \quad (3)$$

and

$$W_{f_1}(\bar{u}) = W_{f_2}((u \oplus \mathbf{1}_n)\Lambda^T) = W_{f_2}(u\Lambda^T \oplus e_n) = W_{f_2}(w \oplus e_n) = \frac{1}{\sqrt{2}}[W_g(w') - (-1)^{w_n}W_h(w')], \quad (4)$$

where $w' = (w_1, \dots, w_{n-1}) \in \mathbb{F}_2^{n-1}$. It follows from Lemma 1, equalities (3) and (4) that

$$\begin{aligned} N_f(u) &= \frac{W_{f \oplus \sigma_2}(u) + W_{f \oplus \sigma_2}(\bar{u})}{2} + i \cdot \frac{W_{f \oplus \sigma_2}(u) - W_{f \oplus \sigma_2}(\bar{u})}{2} \\ &= \frac{W_{f_1}(u) + W_{f_1}(\bar{u})}{2} + i \cdot \frac{W_{f_1}(u) - W_{f_1}(\bar{u})}{2} \\ &= \frac{W_g(w')}{\sqrt{2}} + i \cdot (-1)^{w_n} \frac{W_h(w')}{\sqrt{2}}. \end{aligned} \quad (5)$$

Since the matrix Λ is invertible, we have that $w = u\Lambda^T = (w', w_n)$ runs over \mathbb{F}_2^n if u runs all over \mathbb{F}_2^n .

Boolean function $f \in \mathcal{B}_n$ is negabent if and only if $|N_f(u)| = 1$ for all $u \in \mathbb{F}_2^n$. It follows from equality (5) that

$$|2^{\frac{n-1}{2}}W_g(w')|^2 + |2^{\frac{n-1}{2}}W_h(w')|^2 = 2^n, \text{ for all } w' \in \mathbb{F}_2^{n-1}.$$

By Jacobis two-square theorem, it is equivalent to

$$|W_g(w')| = |W_h(w')| = 1, \text{ for all } w' \in \mathbb{F}_2^{n-1},$$

which means that g and h are both bent functions with $(n-1)$ variables. Therefore, (1) is equivalent to (3).

(2) \Leftrightarrow (4): Let $f'(x, y) = f(x) \oplus \sigma_2(x) \oplus \sigma_1(x)y = f(x) \oplus \sigma_2(x) \oplus (\mathbf{1}_n \cdot x)y \in \mathcal{B}_{n+1}$. Then the Walsh-Hadamard transform of $f'(x, y)$ at $(u, v) \in \mathbb{F}_2^{n+1}$, $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2$, is

$$\begin{aligned} W_{f'}(u, v) &= 2^{-\frac{n+1}{2}} \sum_{x \in \mathbb{F}_2^n, y \in \mathbb{F}_2} (-1)^{f'(x, y) + u \cdot x + vy} \\ &= 2^{-\frac{n+1}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \sigma_2(x) + u \cdot x} + (-1)^v 2^{-\frac{n+1}{2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \sigma_2(x) + \mathbf{1}_n \cdot x + u \cdot x} \\ &= \frac{1}{\sqrt{2}}[W_{f \oplus \sigma_2}(u) + (-1)^v W_{f \oplus \sigma_2}(\bar{u})]. \end{aligned}$$

Then, f' is bent if and only if

$$W_{f'}(u, 0) = \frac{1}{\sqrt{2}}[W_{f \oplus \sigma_2}(u) + W_{f \oplus \sigma_2}(\bar{u})] = \pm 1, \text{ for all } u \in \mathbb{F}_2^n,$$

and

$$W_{f'}(u, 1) = \frac{1}{\sqrt{2}}[W_{f \oplus \sigma_2}(u) - W_{f \oplus \sigma_2}(\bar{u})] = \pm 1, \text{ for all } u \in \mathbb{F}_2^n.$$

That is, $|W_{f \oplus \sigma_2}(u)| \neq |W_{f \oplus \sigma_2}(\bar{u})|$ and $W_{f \oplus \sigma_2}(u) \in \{0, \pm\sqrt{2}\}$ for all $u \in \mathbb{F}_2^n$, i.e., $f(x) \oplus \sigma_2(x)$ is semibent. \square

Theorems 1 and 2 demonstrate that negabent functions and bent functions are closely related. Theorem 2 also shows that n -variable negabent functions must be semibent if n is odd.

IV. NEGA SPECTRUM OF NEGABENT FUNCTIONS

In this section, by using these necessary and sufficient conditions for Boolean functions to be negabent, we discuss the nega spectrum distribution of negabent functions.

Lemma 2: Let $f \in \mathcal{B}_n$ be negabent, the values in the nega spectrum of f are of the form:

- (1) if n is even, then $N_f(u) \in \{\pm 1, \pm i\}$;
- (2) if n is odd, then $N_f(u) \in \{\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}\}$.

Proof: (1) If n is even and $f \in \mathcal{B}_n$ is negabent, then it follows from Theorem 1 that $f \oplus \sigma_2$ is bent. Thus, $W_{f \oplus \sigma_2}(u) = \pm 1$ for all $u \in \mathbb{F}_2^n$. By Lemma 1, we have

$$N_f(u) = \begin{cases} W_{f \oplus \sigma_2}(u), & \text{if } W_{f \oplus \sigma_2}(u) = W_{f \oplus \sigma_2}(\bar{u}), \\ i \cdot W_{f \oplus \sigma_2}(u), & \text{if } W_{f \oplus \sigma_2}(u) \neq W_{f \oplus \sigma_2}(\bar{u}), \end{cases}$$

for all $u \in \mathbb{F}_2^n$. Therefore, $N_f(u) \in \{\pm 1, \pm i\}$.

(2) If n is odd and $f \in \mathcal{B}_n$ is negabent, then it follows from Theorem 2 that $f(x) \oplus \sigma_2(x)$ is semibent and $\{|W_{f \oplus \sigma_2}(u)|, |W_{f \oplus \sigma_2}(\bar{u})|\} = \{0, \sqrt{2}\}$ for all $u \in \mathbb{F}_2^n$. By Lemma 1, we have

$$N_f(u) = \frac{1+i}{2} \cdot W_{f \oplus \sigma_2}(u) + \frac{1-i}{2} \cdot W_{f \oplus \sigma_2}(\bar{u}),$$

thus, $N_f(u) \in \{\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}\}$. □

Lemma 2 shows that the nega spectrum of negabent function has at most 4 values. This leads to a natural question of determining the nega spectrum distribution of negabent functions.

Theorem 3: Let n be even integer and $f \in \mathcal{B}_n$ be negabent, then the nega spectrum distribution of f is

$$\begin{cases} 1, & 2^{n-2} + 2^{\frac{n}{2}-1} & \text{times,} \\ -1, & 2^{n-2} - 2^{\frac{n}{2}-1} & \text{times,} \\ i, & 2^{n-2} & \text{times,} \\ -i, & 2^{n-2} & \text{times,} \end{cases} \quad \text{or} \quad \begin{cases} 1, & 2^{n-2} - 2^{\frac{n}{2}-1} & \text{times,} \\ -1, & 2^{n-2} + 2^{\frac{n}{2}-1} & \text{times,} \\ i, & 2^{n-2} & \text{times,} \\ -i, & 2^{n-2} & \text{times.} \end{cases}$$

Proof: If n is an even integer and $f \in \mathcal{B}_n$ is negabent, then by Theorem 1, we have $f \oplus \sigma_2$ is bent. It is well known that the dual of the bent function $f \oplus \sigma_2$, $\widetilde{f \oplus \sigma_2}$, is also bent. By Lemma 1, we can get that

$$\begin{aligned} N_f(u) &= \frac{(-1)^{\widetilde{f \oplus \sigma_2}(u)} + (-1)^{\widetilde{f \oplus \sigma_2}(\bar{u})}}{2} + i \cdot \frac{(-1)^{\widetilde{f \oplus \sigma_2}(u)} - (-1)^{\widetilde{f \oplus \sigma_2}(\bar{u})}}{2} \\ &= \begin{cases} (-1)^{\widetilde{f \oplus \sigma_2}(u)}, & \text{if } \widetilde{f \oplus \sigma_2}(\bar{u}) = \widetilde{f \oplus \sigma_2}(u), \\ i \cdot (-1)^{\widetilde{f \oplus \sigma_2}(u)}, & \text{if } \widetilde{f \oplus \sigma_2}(\bar{u}) \neq \widetilde{f \oplus \sigma_2}(u), \end{cases} \end{aligned} \quad (6)$$

for all $u \in \mathbb{F}_2^n$.

For $0 \leq i, j \leq 1$, denote

$$S_{i,j} = |\{u \in \mathbb{F}_2^n \mid \widetilde{f \oplus \sigma_2}(u) = i, \widetilde{f \oplus \sigma_2}(\bar{u}) = j\}|. \quad (7)$$

Recall that $C_{\widetilde{f \oplus \sigma_2}}(\alpha) = \sum_{u \in \mathbb{F}_2^n} (-1)^{\widetilde{f \oplus \sigma_2}(u) \oplus \widetilde{f \oplus \sigma_2}(u \oplus \alpha)} = 0$ for $\alpha \neq \mathbf{0}_n$ since $\widetilde{f \oplus \sigma_2}$ is bent, in particular

$$C_{\widetilde{f \oplus \sigma_2}}(\mathbf{1}_n) = \sum_{u \in \mathbb{F}_2^n} (-1)^{\widetilde{f \oplus \sigma_2}(u) \oplus \widetilde{f \oplus \sigma_2}(\bar{u})} = 0,$$

which implies

$$S_{0,0} + S_{1,1} = 2^{n-1}, \quad (8)$$

$$S_{0,1} + S_{1,0} = 2^{n-1}. \quad (9)$$

Clearly $S_{1,0} = |\{\bar{u} \in \mathbb{F}_2^n | \widetilde{f \oplus \sigma_2}(\bar{u}) = 1, \widetilde{f \oplus \sigma_2}(u) = 0\}| = |\{u \in \mathbb{F}_2^n | \widetilde{f \oplus \sigma_2}(\bar{u}) = 1, \widetilde{f \oplus \sigma_2}(u) = 0\}| = S_{0,1}$. Immediately, it follows from equality (9) that $S_{0,1} = S_{1,0} = 2^{n-2}$. By equality (6),

$$|\{u \in \mathbb{F}_2^n | N_f(u) = i\}| = |\{u \in \mathbb{F}_2^n | N_f(u) = -i\}| = 2^{n-2}. \quad (10)$$

Since $\widetilde{f \oplus \sigma_2}$ is bent, we have $\text{wt}(\widetilde{f \oplus \sigma_2}) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. It is obvious that $\text{wt}(\widetilde{f \oplus \sigma_2}) = S_{1,0} + S_{1,1} = 2^{n-2} + S_{1,1}$. Thus by equality (8),

$$\begin{cases} S_{0,0} = 2^{n-2} + 2^{\frac{n}{2}-1}, \\ S_{1,1} = 2^{n-2} - 2^{\frac{n}{2}-1}, \end{cases} \quad \text{or} \quad \begin{cases} S_{0,0} = 2^{n-2} - 2^{\frac{n}{2}-1}, \\ S_{1,1} = 2^{n-2} + 2^{\frac{n}{2}-1}. \end{cases} \quad (11)$$

Combining equalities (6), (7), (10), and (11), we get the desired result. \square

Theorem 4: Let n be odd integer and $f \in \mathcal{B}_n$ be negabent, then the nega spectrum distribution of f is

$$\begin{cases} \frac{1+i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} & \text{times}, \\ \frac{1-i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} & \text{times}, \\ \frac{-1+i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} & \text{times}, \\ \frac{-1-i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} & \text{times}, \end{cases} \quad \text{or} \quad \begin{cases} \frac{1+i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} & \text{times}, \\ \frac{1-i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} & \text{times}, \\ \frac{-1+i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} & \text{times}, \\ \frac{-1-i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} & \text{times}. \end{cases}$$

Proof: If n is odd and $f \in \mathcal{B}_n$ is negabent, then by Theorem 2, we have

$$(f \oplus \sigma_2)(x_1, \dots, x_{n-1}, x_1 \oplus x_2 \oplus \dots \oplus x_n) = (1 \oplus x_n)g(x_1, \dots, x_{n-1}) \oplus x_n h(x_1, \dots, x_{n-1}),$$

where both g and h are bent functions with $(n-1)$ variables. By equality (5), we have

$$N_a = |\{u \in \mathbb{F}_2^n | N_f(u) = a\}| = |\{(w', w_n) \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2 | \frac{W_g(w')}{\sqrt{2}} + i \cdot (-1)^{w_n} \frac{W_h(w')}{\sqrt{2}} = a\}|, \quad (12)$$

where $a \in \{\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}\}$.

Because g is a bent function of $(n-1)$ variables, we have $|\{w' \in \mathbb{F}_2^{n-1} | W_g(w') = 1\}| = 2^{n-2} \pm 2^{\frac{n-1}{2}-1}$. If $|\{w' \in \mathbb{F}_2^{n-1} | W_g(w') = 1\}| = 2^{n-2} + 2^{\frac{n-1}{2}-1}$, then $|\{w' \in \mathbb{F}_2^{n-1} | W_g(w') = -1\}| = 2^{n-2} - 2^{\frac{n-1}{2}-1}$. For any $w' \in \{w' \in \mathbb{F}_2^{n-1} | W_g(w') = 1\}$, we can get that

$$\frac{W_g(w')}{\sqrt{2}} + i \cdot (-1)^{w_n} \frac{W_h(w')}{\sqrt{2}} = \begin{cases} \frac{1+i \cdot W_h(w')}{\sqrt{2}}, & \text{if } w_n = 0, \\ \frac{1-i \cdot W_h(w')}{\sqrt{2}}, & \text{if } w_n = 1, \end{cases}$$

Since $W_h(w') = \pm 1$ for all $w' \in \mathbb{F}_2^{n-1}$, we have

$$N_{\frac{1+i}{\sqrt{2}}} = N_{\frac{1-i}{\sqrt{2}}} = 2^{n-2} + 2^{\frac{n-1}{2}-1}.$$

Because of $|\{w' \in \mathbb{F}_2^{n-1} | W_g(w') = -1\}| = 2^{n-2} - 2^{\frac{n-1}{2}-1}$, we can also get that

$$N_{\frac{-1+i}{\sqrt{2}}} = N_{\frac{-1-i}{\sqrt{2}}} = 2^{n-2} - 2^{\frac{n-1}{2}-1}.$$

Combining with equality (12), we can conclude that the nega spectrum of f in this case is

$$\left\{ \begin{array}{ll} \frac{1+i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} \text{ times,} \\ \frac{1-i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} \text{ times,} \\ \frac{-1+i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} \text{ times,} \\ \frac{-1-i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} \text{ times.} \end{array} \right.$$

Similarly, if $|\{w' \in \mathbb{F}_2^{n-1} | W_g(w') = 1\}| = 2^{n-2} - 2^{\frac{n-1}{2}-1}$ and $|\{w' \in \mathbb{F}_2^{n-1} | W_g(w') = -1\}| = 2^{n-2} + 2^{\frac{n-1}{2}-1}$, we can get the nega spectrum of f as follows

$$\left\{ \begin{array}{ll} \frac{1+i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} \text{ times,} \\ \frac{1-i}{\sqrt{2}}, & 2^{n-2} - 2^{\frac{n-1}{2}-1} \text{ times,} \\ \frac{-1+i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} \text{ times,} \\ \frac{-1-i}{\sqrt{2}}, & 2^{n-2} + 2^{\frac{n-1}{2}-1} \text{ times.} \end{array} \right.$$

This completes the proof. \square

V. CONSTRUCTION OF BENT-NEGABENT FUCTIONS WITH MAXIMUM ALGEBRAIC DEGREE

It is well known that the maximum degree of a bent function on n variables is $\frac{n}{2}$ (for even n) [1] and the maximum degree of a negabent function on n variables is $\lceil \frac{n}{2} \rceil$ (for any integer n) [7]. But, so far all the known general constructions of bent-negabent functions on n variables produce functions with algebraic degrees less than or equal to $\frac{n}{4} + 1$, where n is any positive integer divisible by 4 (see [5], [7], [8]).

Throughout this section, let $n = 2m$ be any even integer greater than or equal to 4, and h be a quadratic bent fuction defined as $h(x) = \bigoplus_{i=1}^m x_i x_{m+i}$ for all $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$. It is known that any quadratic bent function of n variables is equivalent to $h(x)$ [9]. Since $\sigma_2(x)$ is a quadratic bent function [10], then there exist $A \in GL(n, \mathbb{F}_2)$, $b, u \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that

$$\sigma_2(x) = h(xA \oplus b) \oplus u \cdot x \oplus \epsilon. \quad (13)$$

In the sequel, we always assume that $\sigma_2(x)$ is of the above form as (13).

In [7], Stănică *et al.* provided a strategy to construct bent-negabent functions.

Lemma 3: ([7]) Suppose that both $f \in \mathcal{B}_n$ and $f \oplus h$ are bent functions. Then $f' \in \mathcal{B}_n$ defined by

$$f'(x) = f(xA \oplus b) \oplus \sigma_2(x), \quad x \in \mathbb{F}_2^n,$$

is a bent-negabent function.

Let $f \in \mathcal{B}_n$ be a Boolean function of the form

$$f(x, y) = x \cdot \pi(y) \oplus g(y), \quad x, y \in \mathbb{F}_2^m, \quad (14)$$

where “ \cdot ” denotes the inner product in \mathbb{F}_2^m , $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$, and $g : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$. Then the function f is bent if and only if π is a permutation. The whole set of such bent functions forms the well-known *Maierana-McFarland class*. It is shown in [5] that the degree of a Maierana-McFarland-type bent-negabent functions on n variables is at most $\frac{n}{2} - 1$ for $n \geq 8$.

For every positive integer m , the vector space \mathbb{F}_2^m can be endowed with the structure of the finite field \mathbb{F}_{2^m} . Any permutation on \mathbb{F}_2^m can be identified with a permutation of \mathbb{F}_{2^m} . A polynomial $F(X)$ over \mathbb{F}_{2^m} is called a *complete*

mapping polynomial if both $F(X)$ and $F(X) + X$ are permutation polynomials of \mathbb{F}_{2^m} . Combining the above Lemma 3 and complete mapping polynomials over \mathbb{F}_{2^m} , Stănică *et al.* gave a method to construct bent-negabent functions from Maiorana-McFarland bent functions $f_F(x) = \pi_F(x_1, \dots, x_m) \cdot (x_{m+1}, \dots, x_n)$, where π_F denotes the permutation on \mathbb{F}_2^m induced by a complete mapping polynomial $F(X) \in \mathbb{F}_{2^m}[X]$. However, the degrees of the bent-negabent functions they constructed are equal to $\deg(\pi_F) + 1$, and there are only few known results on the complete mapping polynomials with high degrees over \mathbb{F}_{2^m} . They could prove that there exist bent-negabent functions on $n = 12l$ variables with algebraic degree $\frac{n}{4} + 1 = 3l + 1$, since there exist complete mapping polynomials on \mathbb{F}_{2^m} of degrees $3l$, where $m = 6l$ and $l \geq 2$ (see [7], [11]).

In fact, if $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ is a mapping such that $\pi(y)$ and $\pi(y) \oplus y$ are permutations, from Maiorana-McFarland bent functions we can construct infinite class of bent-negabent functions on n variables of degree ranging from 2 to $\frac{n}{2}$. More precisely, we get the following results:

- 1) We calculate the concrete value of A in equality (13);
- 2) We show that there exists mapping $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ such that $\pi(y)$ and $\pi(y) \oplus y$ are permutations and give two methods to get these mappings for any $m \geq 2$;
- 3) Using the linear transform A and such mapping π , we get bent-negabent functions on n variables of degree arranging from 2 to $\frac{n}{2}$ for any even $n \geq 4$. Note that the maximum degree of our bent-negabent functions on n variables is equal to $\frac{n}{2}$. Thus, we answer the Open Problems 1 and 2.

A. The concrete values of A , b , u and ϵ

By transforming the quadratic form σ_2 into its canonical form, we can obtain that the concrete values of $A = (a_{ij})_{n \times n} \in GL(n, \mathbb{F}_2)$, $u = (u_1, u_2, \dots, u_n)$, $b = (b_1, b_2, \dots, b_n) \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ in equality (13) are

- (1) $a_{ii} = 1$ if $1 \leq i \leq n$, $a_{ij} = a_{i,m+j} = a_{m+i,j} = a_{m+i,m+j} = 1$ if $2 \leq i \leq m$ and $1 \leq j \leq i - 1$, and $a_{ij} = 0$ otherwise;
- (2) $u = \mathbf{0}_n$;
- (3) $b_{2i} = b_{m+2i} = 1$ if $1 \leq i \leq \lfloor \frac{m}{2} \rfloor$, and $b_j = 0$ otherwise;
- (4) $\epsilon = 1$ if $m \equiv 2, 3 \pmod{4}$, and $\epsilon = 0$ if $m \equiv 0, 1 \pmod{4}$.

Define matrix $S_m = (s_{ij})_{m \times m}$ over \mathbb{F}_2 by

$$s_{ij} = \begin{cases} 1, & \text{if } 2 \leq i \leq m, 1 \leq j \leq i - 1; \\ 0, & \text{otherwise.} \end{cases}$$

Then, the $n \times n$ matrix A can be written as

$$A = \begin{pmatrix} S_m \oplus I_m & S_m \\ S_m & S_m \oplus I_m \end{pmatrix},$$

and $A^{-1} = A$.

B. The existence of mapping π

In this subsection, we first explain that there exists mapping $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ such that $\pi(y)$ and $\pi(y) \oplus y$ are permutations for any $m \geq 2$ from the perspective of the complete mapping polynomial over finite field \mathbb{F}_{2^m} . And then introduce two methods to obtain the mapping π directly from the vector space \mathbb{F}_2^m .

If $\sigma(x)$ is a complete mapping polynomial over \mathbb{F}_{2^m} , then the corresponding permutation $\sigma'(x)$ on \mathbb{F}_2^m satisfies $\sigma'(x)$ and $\sigma'(x) \oplus x$ are both permutations. Trivial examples of complete mapping polynomials are the linear polynomials $\sigma(x) = ax$ with $a \neq 0, -1$. If $m \geq 3$, there exist complete mapping polynomials of \mathbb{F}_{2^m} of reduced degree > 1 . For details on complete mapping polynomials we refer to [12]. Thus, there exists mapping $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ such that both $\pi(y)$ and $\pi(y) \oplus y$ are permutations for any $m \geq 2$.

In what follows, we introduce two methods to obtain the linear permutation $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ such that $\pi(y) \oplus y$ is also permutation for any $m \geq 2$. Define the mapping $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ as $\pi(y) = yM$, where $y = (y_1, y_2, \dots, y_m) \in \mathbb{F}_2^m$. If we can find $m \times m$ matrix M over \mathbb{F}_2 such that M and $M \oplus I_m$ have full rank m , then we get the desired linear permutation π .

If $m = 2$, there are two matrices satisfy the conditions:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Using exhaustive computer search, we found that there are 48 matrices satisfying the conditions for $m = 3$, and 5824 matrices satisfying the conditions for $m = 4$. For example,

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

and

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Method 1. For any even $m \geq 4$, Parker and Pott gave a method to construct $m \times m$ symmetric matrix M over \mathbb{F}_2 such that M and $M \oplus I_m$ have rank m in Section 3 of [4]. To save space, here we will not give the detail.

Method 2. An $m \times m$ block matrix P is said to be *block diagonal matrix* if it has main diagonal blocks square matrices such that the off-diagonal blocks are zero matrices, i.e., P has the form

$$P = \begin{pmatrix} P_1 & 0 & \cdots & 0 \\ 0 & P_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P_t \end{pmatrix},$$

where P_j , $1 \leq j \leq t$, is a square matrix of order k_j , and $k_1 + \cdots + k_t = m$. It can be indicated as $\text{diag}(P_1, P_2, \dots, P_t)$. Any square matrix can trivially be considered a block diagonal matrix with only one block.

For the determinant of block diagonal matrix P , the following property holds

$$\det(P) = \prod_{i=1}^t \det(P_i).$$

By this property of diagonal matrix, we can easily get the following recursive construction.

Lemma 4: Let $t \geq 2$ and M_j be a square matrix of order k_j such that M_j and $M_j \oplus I_{k_j}$ have full rank for any $1 \leq j \leq t$. If $k_1 + \cdots + k_t = m$, then the matrix $M = \text{diag}(M_1, M_2, \dots, M_t)$ and $M \oplus I_m$ have rank m .

As mentioned before, for $m = 2, 3$, there exists matrix M such that both M and $M \oplus I_m$ have full rank. Thus, for any $m \geq 2$, we can get matrix M such that M and $M \oplus I_m$ have full rank by Lemma 4. Therefore, the linear permutation $\pi(y) = yM$ has been obtained.

C. Construction for infinite class of bent-negabent functions

If $f \in \mathcal{B}_n$ is a bent function, then the function given by

$$f(x \cdot C \oplus \alpha) \oplus \beta \cdot x \oplus \zeta, \quad \text{where } C \in GL(n, \mathbb{F}_2), \alpha, \beta \in \mathbb{F}_2^n, \zeta \in \mathbb{F}_2, \quad (15)$$

is also bent. All the functions in (15) is called a *complete class*. Specifically, it is said to be Maiorana-McFarland complete class if f belongs to Maiorana-McFarland class in (14).

Counterexamples show that these operations generally do not preserve the negabent property of a Boolean function. Indeed if $GL(n, \mathbb{F}_2)$ is replaced by $O(n, \mathbb{F}_2)$, the orthogonal group of $n \times n$ matrices over \mathbb{F}_2 , the negabent property is still preserved.

Lemma 5: ([5]) Let $f, g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be two Boolean functions. Suppose that f and g are related by $g(x) = f(x \cdot O \oplus \alpha) \oplus \beta \cdot x \oplus \zeta$, where O is an $n \times n$ orthogonal matrix over \mathbb{F}_2 , $\alpha, \beta \in \mathbb{F}_2^n$, and $\zeta \in \mathbb{F}_2$. Then, if f is bent-negabent, g is also bent-negabent.

Now, we are ready to construct $2m$ -variable bent-negabent functions of degree ranging from 2 to m .

Theorem 5: Define $f \in \mathcal{B}_n$ by

$$f(x, y) = x \cdot \pi(y) \oplus g(y), \quad x, y \in \mathbb{F}_2^m,$$

where $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ is a mapping such that $\pi(y)$ and $\pi(y) \oplus y$ are permutations and $g \in \mathcal{B}_m$. Then

$$f'(x, y) = f((x, y) \cdot OA \oplus \alpha) \oplus \beta \cdot x \oplus \zeta \quad (16)$$

is a bent-negabent function with $\deg(f') = \deg(f)$, for any $\alpha, \beta \in \mathbb{F}_2^n$, $\zeta \in \mathbb{F}_2$, and any $n \times n$ orthogonal matrix O over \mathbb{F}_2 .

Proof: If $\pi(y)$ and $\pi(y) \oplus y$ are permutations on \mathbb{F}_2^m , we have that $f(x, y)$ and $f(x, y) \oplus h(x, y) = f(x, y) \oplus x \cdot y$ are both Maiorana-McFarland bent functions. It follows from Lemma 3 and Corollary 1 that $f((x, y) \cdot A \oplus b)$ is a bent-negabent function. Applying Lemma 5 to $f((x, y) \cdot A \oplus b)$, we have that $f((x, y) \cdot OA \oplus \alpha) \oplus \beta \cdot x \oplus \zeta$ is also a bent-negabent function for any $\alpha, \beta \in \mathbb{F}_2^n$, $\zeta \in \mathbb{F}_2$, and any $n \times n$ orthogonal matrix O over \mathbb{F}_2 .

Since the algebraic degree is an affine invariant, we have $\deg(f') = \deg(f)$. □

Note that we are free to choose g . Specifically if taking $g \in \mathcal{B}_m$ with $\deg(g) = m$, one has $\deg(f') = \deg(f) = m$. It is well known that the maximum degree of bent function in $2m$ variables is m . Then, the maximum degree of bent-negabent function in $2m$ variables is less than or equal to m . Our construction can reach the maximal degree, so the bound is tight. Therefore, the following result holds.

Corollary 2: Let n be even and $f \in \mathcal{B}_n$. If f is bent-negabent, then the algebraic degree of f is at most $\frac{n}{2}$. And the bent-negabent function f' given by (16) can achieve the maximal algebraic degree if $\deg(g) = m$ or $\deg(\pi) = m - 1$.

Remark 1: Since the degree of a Maiorana-McFarland-type bent-negabent function on n variables is at most $\frac{n}{2} - 1$ for $n \geq 8$ (see [5]), the functions constructed by Theorem 5 may not in the Maiorana-McFarland class, but belong to the Maiorana-McFarland complete class.

The dual also preserve the bent-negabent function property.

Lemma 6: ([4]) If f is a bent-negabent function, then its dual is again bent-negabent.

Lemma 7: ([9]) The algebraic degrees of any n -variable bent function f and of its dual \tilde{f} satisfy:

$$\frac{n}{2} - \deg(f) \geq \frac{\frac{n}{2} - \deg(\tilde{f})}{\deg(\tilde{f}) - 1}.$$

It follows from Lemma 7 that the degree of \tilde{f} , $\deg(\tilde{f})$, is also equal to $\frac{n}{2}$ if f is an n -variable bent function with $\deg(f) = \frac{n}{2}$. Combining Lemma 6 and Lemma 7, we have the following corollary.

Corollary 3: Let $p(x) \in \mathcal{B}_n$ be a bent-negabent function with degree m obtained from Theorem 5. Then its dual is again bent-negabent with degree m .

D. Examples of n -variable bent-negabent functions with maximum degree for $n = 8$ and $n = 10$

Example 1: Take $m = 4$, $n = 2m = 8$, $\pi(y) = yM$ with matrix

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

and $g(y) = y_1y_2y_3y_4$ in Theorem 5. It is easy to check that matrices M and $M \oplus I_4$ have rank 4. Then

$$\pi(y) = yM = (y_2 \oplus y_4, y_1 \oplus y_3, y_2, y_1),$$

and

$$f(x, y) = x \cdot \pi(y) \oplus g(y) = x_1 \cdot (y_2 \oplus y_4) \oplus x_2 \cdot (y_1 \oplus y_3) \oplus x_3 \cdot y_2 \oplus x_4 \cdot y_1 \oplus y_1y_2y_3y_4.$$

The linear transformation matrix A is equal to

$$A = \begin{pmatrix} S_4 \oplus I_4 & S_4 \\ S_4 & S_4 \oplus I_4 \end{pmatrix}, \text{ where } S_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Let $O = I_n$, $\alpha = \beta = \mathbf{0}_n$ and $\zeta = 0$. Then the function $f'(x, y) = f((x, y)A) = x_2x_3x_4y_4 \oplus x_2x_3y_3y_4 \oplus x_2x_4y_2y_4 \oplus x_2y_2y_3y_4 \oplus x_3x_4y_1y_4 \oplus x_3y_1y_3y_4 \oplus x_4y_1y_2y_4 \oplus y_1y_2y_3y_4 \oplus x_2x_3y_4 \oplus x_2x_4y_4 \oplus x_2y_2y_4 \oplus x_2y_3y_4 \oplus x_3x_4y_4 \oplus x_3y_1y_4 \oplus x_3y_3y_4 \oplus x_4y_1y_4 \oplus x_4y_2y_4 \oplus y_1y_2y_4 \oplus y_1y_3y_4 \oplus y_2y_3y_4 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1y_2 \oplus x_1y_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2y_1 \oplus x_3y_1 \oplus x_3y_4 \oplus x_4y_2 \oplus x_4y_4 \oplus y_1y_3 \oplus y_2y_3 \oplus y_3y_4 \oplus x_2 \oplus x_3 \oplus x_4 \oplus y_2 \oplus y_3$ is bent-negabent and $\deg(f') = 4$.

Example 2: Take $m = 5$, $n = 2m = 10$, $\pi(y) = yM$ with matrix

$$M = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}, \text{ where } M_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } M_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

and $g(y) = y_1y_2y_3y_4y_5 \oplus y_2y_3y_4y_5$. It is easy to check that matrices M and $M \oplus I_5$ have rank 5. Then

$$\pi(y) = yM = (y_1 \oplus y_2, y_1, y_4 \oplus y_5, y_3 \oplus y_4, y_3),$$

and

$$f(x, y) = x \cdot \pi(y) \oplus g(y) = x_1(y_1 \oplus y_2) \oplus x_2y_1 \oplus x_3(y_4 \oplus y_5) \oplus x_4(y_3 \oplus y_4) \oplus x_5y_3 \oplus y_1y_2y_3y_4y_5 \oplus y_2y_3y_4y_5.$$

The linear transformation matrix A is equal to

$$A = \begin{pmatrix} S_5 \oplus I_5 & S_5 \\ S_5 & S_5 \oplus I_5 \end{pmatrix}, \text{ where } S_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Therefore, the function $f'(x, y) = f((x, y)A) = (x_2 \oplus y_1)(x_3x_4x_5y_5 \oplus x_3x_4y_4y_5 \oplus x_3x_5y_3y_5 \oplus x_3y_3y_4y_5 \oplus x_4x_5y_2y_5 \oplus x_4y_2y_4y_5 \oplus x_5y_2y_3y_5 \oplus y_2y_3y_4y_5 \oplus x_3x_4y_5 \oplus x_3x_5y_5 \oplus x_3y_3y_5 \oplus x_3y_4y_5 \oplus x_4x_5y_5 \oplus x_4y_2y_5 \oplus x_4y_4y_5 \oplus x_5y_2y_5 \oplus x_5y_3y_5 \oplus y_2y_3y_5 \oplus y_2y_4y_5 \oplus y_3y_4y_5 \oplus x_3y_5 \oplus x_4y_5 \oplus x_5y_5 \oplus y_2y_5 \oplus y_3y_5 \oplus y_4y_5) \oplus x_1x_2 \oplus x_1y_1 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2y_3 \oplus x_2y_4 \oplus x_3x_5 \oplus x_3y_2 \oplus x_3y_4 \oplus x_4x_5 \oplus x_4y_2 \oplus x_4y_3 \oplus x_4y_4 \oplus x_4y_5 \oplus x_5y_2 \oplus x_5y_4 \oplus y_1y_2 \oplus y_1y_5 \oplus y_2y_3 \oplus y_2y_4 \oplus y_2y_5 \oplus y_3y_5 \oplus y_4y_5 \oplus x_3 \oplus x_5 \oplus y_5$ is bent-negabent and $\deg(f') = 5$.

REFERENCES

- [1] O.S. Rothaus, "On bent functions," Journal of Combinatorial Theory, Ser. A, vol. 20, no. 3, pp. 300-305, 1976.
- [2] M.G. Parker, "The constabent properties of Golay-Davis-Jedwab sequences," In proceedings of IEEE International Symposium on Information Theory, 2000.
- [3] C. Riera and M.G. Parker, "Generalized bent criteria for Boolean functions (I)," IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, 2006.
- [4] M.G. Parker and A. Pott, "On Boolean functions which are bent and negabent," Lecture Notes in Computer Science, vol. 4893, pp. 9-23, 2007.
- [5] K.-U. Schmidt, M.G. Parker and A. Pott, "Negabent functions in the Maiorana- McFarland class," In proceedings of SETA 2008, Lecture Notes in Computer Science, vol. 5203, pp. 390-402, 2008.
- [6] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay and S. Maitra, "Nega-Hadamard transform, bent and negabent functions," In proceedings of SETA 2010, Lecture Notes in Computer Science, vol. 6338, pp. 359-372, 2010.
- [7] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, and S. Maitra, "Investigations on bent and negabent functions via the nega-Hadamard transform," IEEE Trans. Inf. Theory, vol. 58, no. 6, pp. 4064-4072, 2012.
- [8] S. Sarkar, "Characterizing negabent Boolean functions over finite fields," In proceedings of SETA 2012, Lecture Notes in Computer Science, vol. 7280, pp. 77-88, 2012.
- [9] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes," Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering," Cambridge University Press (Peter Hammer and Yves Crama editors), pages 257-397, 2010.
- [10] P. Savicky, "On the bent boolean functions that are symmetric," European Journal of Combinatorics, vol. 15, no. 4, pp. 407-410, 1994.
- [11] Y. Laigle-Chapuy, "Permutation polynomials and applications to coding theory," Finite Fields and Their Applications, vol. 13, pp. 58-70, 2007.
- [12] H. Niederreiter and K.H. Robinson, "Complete mappings of finite fields," J. Austral. Math. Soc. (Series A), vol. 33, 197-212, 1982.